[Separate counsel for each defendant joining this joint brief are listed on the signature page]

**UNITED STATES DISTRICT COURT**

**NORTHERN DISTRICT OF CALIFORNIA**

**SAN JOSE DIVISION**

WINSTON SMITH; JANE DOE I; and JANE DOE II, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

FACEBOOK, INC.; AMERICAN CANCER SOCIETY, INC.; AMERICAN SOCIETY OF CLINICAL ONCOLOGY, INC.; MELANOMA RESEARCH FOUNDATION; ADVENTIST HEALTH SYSTEM; BJC HEALTHCARE; CLEVELAND CLINIC; and UNIVERSITY OF TEXAS—MD ANDERSON CANCER CENTER,

Defendants.

Case No. 5:16-cv-01282-EJD

**DEFENDANTS' JOINT NOTICE OF MOTION AND MOTION TO DISMISS THE COMPLAINT**

Date: November 17, 2016
Time: 9:00 a.m.
Dept.: 4, 5th Floor
Before: Hon. Edward J. Davila

**TABLE OF CONTENTS**

## TABLE OF AUTHORITIES

**Cases**

**Statutes**



**Other Authorities**

## NOTICE OF MOTION AND MOTION

PLEASE TAKE NOTICE that on November 17, 2016, at 9:00 a.m., before the Honorable Edward J. Davila of the United States District Court for the Northern District of California, Courtroom 4, 280 South 1st Street, San Jose, California, Defendants Facebook, Inc. ("Facebook"), American Cancer Society, Inc. ("ACS"), American Society of Clinical Oncology, Inc. ("ASCO"), Melanoma Research Foundation ("MRF"), Adventist Health System Sunbelt Healthcare Corporation ("AHS"), BJC Health System d/b/a BJC HealthCare ("BJC"), Cleveland Clinic of Texas ("Cleveland Clinic"), and University of Texas—MD Anderson Cancer Center ("MD Anderson") (other than Facebook, collectively the "healthcare defendants") will, and hereby do, move this Court pursuant to Federal Rules of Civil Procedure 12(b)(1), 12(b)(2), and 12(b)(6) for an order dismissing the complaint with prejudice.

The motion is based upon this notice of motion; the memorandum of points and authorities in support thereof that follows; the proposed order filed concurrently herewith; the pleadings, records, and papers on file in this action; oral argument of counsel; and any other matters properly before the Court.

## STATEMENT OF ISSUES TO BE DECIDED

1. Should the complaint be dismissed under Rule 12(b)(1) as to all defendants for lack of subject matter jurisdiction?

2. Should the complaint be dismissed under Rule 12(b)(2) as to the healthcare defendants for lack of personal jurisdiction?

3. Should the complaint be dismissed under Rule 12(b)(6) as to all defendants for failure to state a claim?

4. Should the complaint be dismissed as to defendant MD Anderson because MD Anderson has sovereign immunity under the Eleventh Amendment?

## MEMORANDUM OF POINTS AND AUTHORITIES

## INTRODUCTION

This lawsuit is a repackaged version of a case that this Court has already dismissed, albeit with leave to replead: *In re Facebook Internet Tracking Litigation*, 140 F. Supp. 3d 922 (N.D. Cal. 2015) (Davila, J.) ("*Facebook Internet*"). The claims in this case, filed by the same plaintiffs' law firm, are similarly based on Facebook's receipt and use of information that is sent from users about their visits to third-party websites. The main difference between the two cases is that here, plaintiffs attempt to bolster and distinguish their claims by focusing on Facebook's alleged use of what they call "sensitive medical information," and by suing not only Facebook but seven renowned hospitals and nonprofit health organizations. These differences are immaterial: Plaintiffs' claims fail for the same fundamental reasons that those in *Facebook Internet* failed—and several others as well.

Facebook is a free social networking service that allows people to connect and share content. Like countless other websites, Facebook earns revenue by allowing third parties to display ads to people who use Facebook's service around the world. To make this advertising as relevant and interesting as possible, Facebook collects information about people's browsing activities, mainly on Facebook but also on third-party websites that host Facebook tools and features. Facebook shares this information in aggregated form with advertisers, who then use it to target their ads to different categories of people; Facebook does *not* share personally-identifying information about specific people. Plaintiffs appear to recognize that these processes allow the Internet to operate as it does; that Facebook fully discloses these practices to all of its users when they sign up for the service; and that it specifically offers people the opportunity to opt out of targeted advertising. Instead of opting out, however, plaintiffs filed this lawsuit. Three independent and overarching reasons compel dismissal.

First, because plaintiffs have not alleged any concrete harm as a result of defendants' conduct, they lack standing to pursue each of their claims. Plaintiffs cannot obtain standing merely by alleging bare statutory violations; that argument is foreclosed by the Supreme Court's recent decision in *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016). And their allegation that they

suffered "economic damage"—based on the theoretical value of their information in the advertising market—fails for the same reason that it did in *Facebook Internet*: They do not (and cannot) allege "that they personally lost the opportunity to sell their information or that the value of their information was somehow diminished" by defendants. 140 F. Supp. 2d at 931-32.

Second, plaintiffs concede that when they signed up for Facebook, they affirmatively attested to having reviewed and consented to Facebook's Data Policy and Cookie Use page, both of which are attached to the complaint. These pages clearly disclose that Facebook "collect[s] . . . information about the websites . . . you visit"; receives information from "*all across the Internet and mobile ecosystem*"; "use[s] *all* of the information we have about you to show you relevant ads"; and provides "third parties . . . with information about the reach and effectiveness of their advertising." Although plaintiffs' consent to Facebook's policies is independently sufficient to bar their claims, the healthcare defendants' websites likewise contain disclosures (also cited in the complaint) about the tracking of users' browsing activities, and specifically direct users to consult the privacy policies of third-party sites for information about data collection. Plaintiffs' concessions on this subject doom their complaint.

Third, plaintiffs' own allegations belie any notion that they have been "wiretapped." Plaintiffs allege that their browsers sent two *separate* communications when they interacted with the healthcare sites: one to the healthcare defendants (the search terms they entered or the links they clicked) and one to Facebook (URL addresses sent from "the user's web-browser . . . to Facebook's server"). Facebook plays no role in the first communication, and the healthcare defendants play no role in the second. Thus, none of the defendants has "intercepted" any communications; each was a *party* to all of the communications that it received.

At bottom, this lawsuit is simply an attack on the way the Internet works. Despite its incendiary rhetoric, the complaint describes nothing more than the routine receipt and use of data to provide a variety of services (often for free) that people enjoy and want to use—activity that is clearly disclosed to plaintiffs the moment that they signed up for Facebook's service, as well as on the healthcare defendants' sites. And although the healthcare defendants are included in the complaint, plaintiffs know that they do not belong in this case: They allege no facts that could

give rise to personal jurisdiction over those defendants, and expressly state that they *do not know* (and therefore *cannot allege*) whether the healthcare defendants knowingly did anything wrong. For these reasons and others—including that the URLs at issue are *not* "sensitive medical information," and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") is categorically inapplicable here as a matter of law—the case should be dismissed with prejudice.

## BACKGROUND[1]

### A. The Internet and Referer Headers

People navigate the Internet using web browsers (like Google Chrome, Apple Safari, and Microsoft Internet Explorer) that send, receive, and display content on computers or other electronic devices. Compl. ¶¶ 21-23. Every webpage is hosted by a computer server that communicates with browsers and provides them with content from the webpage. *Id.* ¶ 24. The most basic communication between server and browser is a "GET request," a message sent from the browser to the server requesting information for display on the computer or device. *Id.* ¶ 25.

GET requests come in various forms—a person can type information into the navigation bar of his browser, or type information into a search engine hosted by the webpage, or click on a hyperlink. *Id.* For example, when a person types "www.cancer.org" (a site operated by defendant ACS) into his browser's navigation bar, the browser sends a GET request to the server for Cancer.org requesting the homepage of that site. *Id.*

Although a webpage appears on a person's screen as a complete product, it is actually an assembly of independent parts, often including content (like advertisements) that exists on different servers operated by third parties. *Id.* ¶ 30. The website server initially leaves blank the parts of the page that will be filled in by third parties. *Id.* ¶ 31. When a browser sends the website server a GET request to view a page that also contains third-party content, the website server sends code to the browser, directing it to send a different and separate GET request to the third party's server. *Id.* ¶ 32. When the third party receives that GET request, it responds with information to fill in the blank portion of the page. *Id.* Thus, the user's browser sends two

[1] Defendants make no admission as to the veracity of the complaint's allegations.

distinct requests: one to the website server to load its portion of the page, and one to the third party's server to load its content onto that same webpage. *Id.*

Because the third party needs to know where to load the requested content, the GET request sent to the third-party server typically contains the Uniform Resource Locator ("URL") of the webpage being loaded. *Id.* ¶ 33. A URL is generally displayed in an address bar at the top of the browser. It consists of several parts: (1) a protocol identifying the language of the interaction between the browser and the server (*e.g.*, "http://"); (2) the name of the website (*e.g.*, "www.cancer.org"); and (3) when applicable, particular folders and subfolders on the server that the browser has requested for display (*e.g.*, "/cancer/"). *Id.* ¶ 28. When sent to third-party servers, URLs are commonly called "referer headers." *Id.* ¶ 33.

Many webpages contain Facebook content or tools, such as its "Like" button (which people can click to tell their friends that they are fond of a piece of content) and its "Share" button (which allows people to share a piece of content on Facebook). *See id.* ¶ 62. When a person's browser requests a webpage that also contains Facebook content, that browser sends a GET request to Facebook's server along with a referer header telling Facebook where to load the requested content. *Id.* ¶ 35. Importantly, as plaintiffs allege, the referer header is sent from "the user's web-browser . . . to Facebook's server" (*id.* ¶ 50(f)); it is a communication "separate" from "the actual communication" between the browser and the host site (*id.* ¶ 255).

**B. Cookies**

A cookie is a small text file that a server creates and sends to a browser when the two communicate. *Id.* ¶¶ 41-42. The browser stores the file on the person's computer and sends information from the cookie back to the server whenever the browser makes additional requests of the same server. *Id.* By examining the cookie, the server can determine whether it has interacted with this browser before and locate records about its history with that browser. *Id.* ¶¶ 42-43, 45-46, 50, 85. And when the cookie is accompanied by a referer header—that is, when the browser has requested a page with third-party content—the server that receives the cookie can connect the data from the cookie with the URL contained in the referer header to determine

which browser has requested the information. *Id.* Cookies are ubiquitous and widely used on the Internet for many purposes, including security, efficiency, and advertising. *Id.* ¶ 42.

**C. Facebook and its Disclosures**

Facebook is a free social networking service. As discussed above, Facebook uses third-party advertising as a means of revenue, and improves that advertising by using information that it collects about people's activities on Facebook and their visits to some third-party websites. Plaintiffs allege that Facebook uses cookies "to sell advertising that is customized based upon a particular person's Internet communications." *Id.* ¶ 43. They further claim that Facebook sorts people into "154 separate medical categories" based on their interests—for example, a category of "84 million users who have expressed an interest in or like pages related to cancer awareness" and therefore might "have an interest in making donations to cancer causes." *Id.* ¶¶ 89-90 & Ex. E.

Facebook fully discloses its receipt and use of data to everyone who joins Facebook (including to each of the named plaintiffs). Plaintiffs acknowledge that "[o]n sign-up, Facebook requires users to click a green Sign Up button" directly underneath the following text: "By clicking Sign Up, you agree to our Terms and that you have read our Data Policy, including our Cookie Use." *Id.* ¶ 58. The phrases "Terms," "Data Policy," and "Cookie Use" are highlighted in blue and link directly to three disclosures (attached to the complaint). *Id.* ¶ 59, Exs. A-C. Plaintiffs allege that these disclosures "constitute[] a valid contract." *Id.* ¶ 59.

***Statement of Rights and Responsibilities***. In the sign-up process, the phrase "Terms" is hyperlinked to Facebook's Statement of Rights and Responsibilities ("SRR"). *Id.* Ex. A. This disclosure states that "[w]e designed our Data Policy to make important disclosures about . . . how we collect and can use your content and information," and that "[b]y using Facebook Services, you agree that we can collect and use such content and information in accordance with the Data Policy." *Id.* Ex. A at 1, 3.

***Data Policy***. The Data Policy states: "We collect information when you visit or use third-party websites and apps that use our Services," "includ[ing] information about the websites and apps you visit, your use of our Services on those websites and apps, [and] information the

developer or publisher of the app or website provides to you or us." *Id.* Ex. B at 2. It then explains *how* Facebook uses this data: It "work[s] with third party companies" "to improve our advertising and measurement systems so we can show you relevant ads on and off our Services and measure the effectiveness and reach of ads and services." *Id.* Ex. B at 3, 5. Specifically:

> We want our advertising to be as relevant and interesting as the other information you find on our Services. With this in mind, ***we use all of the information we have about you to show you relevant ads.*** We do not share information that personally identifies you . . . with advertising . . . partners unless you give us permission. We may provide these partners with information about the reach and effectiveness of their advertising . . . if we have aggregated the information so that it does not personally identify you. For example, we may tell an advertiser how its ads performed, or how many people viewed their ads or installed an app after seeing an ad, or provide non-personally identifying demographic information (such as 25 year old female . . . ).

*Id.* Ex. B at 5 (emphasis added). Finally, the Data Policy tells people that they can "[l]earn more about advertising on our Services and how you can control how information about you is used to personalize the ads you see"; the phrases "Learn more" and "control" are hyperlinked to pages explaining how people can opt out of targeted advertising. *Id.* Ex. B at 3.

***Cookie Policy.*** The Cookie Policy explains that cookies are "used to understand and deliver ads, make them more relevant to you, and analyze products and services and the use of those products and services." *Id.* Ex. C at 2. Specifically, Facebook and its partners use cookies to "learn whether someone . . . makes a purchase on [an] advertiser's site or installs [an] advertised app"; to determine "how [an ad] performed"; and to "show you an ad based on the websites you visit or the apps you use—*all across the Internet and mobile ecosystem.*" *Id.* (emphasis added). Like the Data Policy, the Cookie Policy tells people that "[y]ou can adjust your ad preferences if you want to control your ad experience on Facebook." *Id.* Ex. C at 4.

**D. The Healthcare Defendants and their Disclosures**

The healthcare defendants are nationally recognized, nonprofit organizations that operate in the healthcare industry. None is based in California or has substantial contacts with it:

- ACS is a nonprofit, community-based voluntary health organization dedicated to eliminating cancer as a major health problem. It is headquartered in Atlanta, Georgia. *See id.* ¶ 10.

- ASCO is one of the world's leading nonprofit professional organizations for physicians and oncology professionals caring for people with cancer. It is headquartered in Virginia. *See id.* ¶ 11.
- MRF is the largest independent nonprofit organization devoted to the support of medical research to find effective treatments for melanoma. It is headquartered in Washington DC. *See id.* ¶ 12.
- AHS is a nonprofit healthcare organization headquartered in Florida. *Id.* ¶ 13. It operates 46 hospital campuses, none of which is in California.
- BJC is a nonprofit healthcare provider based in St. Louis, Missouri. *Id.* ¶ 14. It is the parent organization of Barnes-Jewish Hospital, an affiliated academic training hospital of Washington University School of Medicine and the largest and top-ranked hospital in Missouri.
- Cleveland Clinic is a nonprofit healthcare provider based in Cleveland, Ohio. *Id.* ¶ 15. It is a top-five ranked hospital by U.S. News and World Report and has over five million patient visits to its facilities each year, none of which is located in California.
- MD Anderson is a Texas state agency, a component institution of The University of Texas System, and under the management and control of The Board of Regents of The University of Texas System, who are each appointed by the Governor of the State of Texas.

The healthcare defendants maintain websites that provide a wide variety of information and conveniences to patients, families, employees, medical professionals, medical students, charitable donors, and the public at large. Anyone—patients and non-patients alike—can access these websites to obtain information about the healthcare defendants and about general medical topics. Plaintiffs allege that they have no knowledge about the healthcare defendants' intent or states of mind. *Id.* ¶ 5.

The healthcare defendants go out of their way to inform visitors of the fact that, by its very nature, the Internet cannot promise the same level of privacy as an examination or waiting room. Specifically, they disclose that their websites host third-party content, use first- and third-party cookies, and may utilize or make available to third parties the data collected from individual browsers' interactions with their websites. *See, e.g.*, Compl. ¶¶ 111, 127, 142, 156, 171, 184, 197; *see also id.* Exs. F-L. For example:[2]

[2] MD Anderson is not including arguments about its own privacy policy at this time because its Eleventh Amendment immunity must first be determined as a threshold issue.

- ASCO's Privacy Policy states that "Click Stream Information," including referer headers of pages users view when they visit Cancer.net, may be collected when they visit the site; that Click Stream Information may be collected through third-party cookies and technical devices "that provide a presence on the web page and send back to its home Server (which can belong to the host site, a network advertiser, or some other third party) information from the user's Browser"; and that users should "review the privacy policies of other sites carefully." In addition, ASCO's Privacy Policy advises visitors that "the providers of third party Cookies may have the ability to link your activities on the Website with your browsing activities elsewhere on the Internet." *Id.* Ex. G §§ 4, 13.

- ACS's Privacy Policy notifies people of its use of cookies and advises users to "read the privacy policies of each site you visit to determine what information that site may be collecting about you." *Id.* Ex. F at 5.

- MRF's privacy policy discloses its use of cookies and that "[m]any third-party sites have their own privacy policies that differ from ours." *Id.* Ex. H at 4.

- AHS's privacy policy advises that it uses cookies and instructs users to "review the privacy policies of other sites [that may have a link on AHS's site] carefully before providing any information to such website." *Id.* Ex. I.

- BJC notifies users that "[i]nformation you submit may be routinely shared with . . . organizations working on [BJC's] behalf." *Id.* Ex. J, Terms of Use at 2. It expressly urges users "not to provide any confidential information about [themselves] or [their] health . . . via electronic communication." *Id.* BJC also notifies users about its use of cookies to collect user data. *Id.* ("The first visit you make to the [BJC] Web site places a 'cookie' on your computer. . . . Click here to learn more about opting out of data collection.").

- Cleveland Clinic's privacy policy also advises visitors of its use of first-party cookies, and similarly makes "no guarantee as to security, integrity or confidentiality of any information transmitted to or from this website, or stored within this website." *Id.* Ex. K at 2.

**E. Plaintiffs and their Lawsuit**

The three named plaintiffs claim to be registered users of Facebook who sought out the healthcare defendants' websites. *Id.* ¶¶ 6-8. Plaintiff Winston Smith is a resident of Missouri who communicated with four of the healthcare defendants' websites: cancer.org, cancer.net, melanoma.org, and mdanderson.org. *Id.* ¶¶ 6, 117, 132, 147, 202. Plaintiff Jane Doe is a resident of Kansas who allegedly communicated with Adventist Health System's website, shawneemission.org. *Id.* ¶¶ 7, 161. Plaintiff Jane Doe II is a resident of Missouri who claims to

have communicated with the websites of BJC and Cleveland Clinic: barnesjewish.org and clevelandclinic.org. *Id.* ¶¶ 8, 175, 188.[3]

Plaintiffs claim that when they visited the healthcare defendants' websites, "Facebook acquired, tracked, and used the Plaintiffs' sensitive medical information . . . [for] direct marketing." *Id.* ¶¶ 2-4.[4] They are "without knowledge as to whether the disclosures by the health care Defendants were willful and knowing." *Id.* ¶ 5. Plaintiffs further claim that their "medical information" has economic value in the advertising market (*id.* ¶¶ 53-57), and that they sustained "economic loss associated with the medical information taken without their consent" (*id.* ¶ 304, 331). But they do not allege that this value was diminished by defendants' conduct.

Based on these allegations, plaintiffs bring ten causes of action: (1) violation of the federal Wiretap Act; (2) intrusion upon seclusion; (3) violation of the California Invasion of Privacy Act ("CIPA"); (4) California constitutional invasion of privacy; (5) negligence per se; (6) negligent disclosure of confidential information; (7) breach of the fiduciary duty of confidentiality; (8) breach of the duty of good faith and fair dealing; (9) fraud; and (10) quantum meruit. The first five are asserted against all of the defendants; the sixth and seventh are against only the healthcare defendants; and the last three are against only Facebook.

## ARGUMENT

### I. THE COMPLAINT SHOULD BE DISMISSED UNDER RULE 12(b)(1) BECAUSE THIS COURT LACKS SUBJECT MATTER JURISDICTION.

A suit brought by a plaintiff without Article III standing does not meet the Constitution's "case or controversy" requirement and must be dismissed for lack of subject matter jurisdiction under Rule 12(b)(1). *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 101, 109-10 (1998).

---

[3] The specific URLs allegedly visited by the named plaintiffs on the healthcare defendants' websites—and allegedly received by Facebook—are summarized for the Court's convenience as Exhibit A to this motion. Although plaintiffs make passing references to additional websites maintained by the healthcare defendants (*see, e.g.*, Compl. ¶¶ 157, 235), they fail to allege any facts to show that plaintiffs visited those websites or that URLs from those websites were obtained by Facebook or disclosed by the healthcare defendants.

[4] Unlike in *Facebook Internet*, plaintiffs do not distinguish between activities conducted while they were logged out of Facebook and activities conducted while logged in.

To establish standing under Article III, a plaintiff must show that he "has suffered an 'injury in fact' that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical." *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs., Inc.*, 528 U.S. 167, 180 (2000). "Where, as here, a case is at the pleading stage, the plaintiff must *clearly* allege facts demonstrating each element." *Spokeo*, 136 S. Ct. at 1547 (emphasis added). Plaintiffs have failed to meet this burden as to any of their claims.

**A. Plaintiffs Cannot Rely on a Theory of "Statutory Standing."**

In *Facebook Internet*, the Court dismissed most of the claims (with leave to replead) because the plaintiffs had not sufficiently alleged that Facebook's alleged collection of referer headers had resulted in "concrete and particularized harm," and therefore had not established "constitutional standing." 140 F. Supp. 3d at 932. The Court held, however, that it had jurisdiction over three of the plaintiffs' statutory claims—those brought under the Wiretap Act, the Stored Communications Act, and CIPA—under Ninth Circuit case law holding that "an Article III injury can exist solely by virtue of 'statutes creating legal rights, the invasion of which creates standing.'" *Id.* (quoting *Edwards v. First Am. Corp.*, 610 F.3d 514, 517 (9th Cir. 2010)). This theory of pure "statutory standing"—which the Court examined separately from constitutional standing, *see id.*—is no longer good law, and plaintiffs cannot rely on it here.

In *Spokeo*, the Supreme Court reversed the Ninth Circuit and held that a plaintiff does not "automatically satisf[y] the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right." 136 S. Ct. at 1549. Instead, "*Article III standing requires a concrete injury even in the context of a statutory violation.*" *Id.* (emphasis added). The Court held that the Ninth Circuit, applying *Edwards*, had improperly examined only the "particularized" nature of the statutory rights at issue, and failed to determine whether the plaintiff had shown "concrete" injury resulting from the alleged statutory violation; as the Court explained, "the injury-in-fact requirement requires a plaintiff to allege an injury that is *both* concrete and particularized." *Id.* at 1545 (emphasis added) (internal quotation marks omitted). While *Spokeo* reaffirmed precedents holding that certain "intangible injuries" can qualify as injuries in fact, it emphasized that any such injury must satisfy the

constitutional requirement of concreteness; it must be "*de facto*"—that is, "real" rather than "abstract," "conjectural," or "hypothetical." *Id.* at 1548-50.

Here, plaintiffs have not alleged *any* harm as a result of Facebook's collection and use of referer headers, let alone the kind of harm that "has traditionally been regarded as providing a basis for a lawsuit in English or American courts." *Id.* Plaintiffs allege that they are entitled to recover based on defendants' alleged violations of the Wiretap Act and CIPA (Compl. ¶¶ 294, 321), but they do not allege any concrete injury that flowed from those alleged violations. Instead, they claim only the kind of speculative "economic harm" that, as we discuss next, both this Court and others in this Circuit have uniformly rejected as a basis for standing.

**B. Plaintiffs Have Not Alleged a Concrete Injury.**

Plaintiffs do not allege that they have suffered any physical, mental, intangible, or other form of *non*-economic injury as a result of defendants' alleged conduct. Although they characterize their data as "sensitive" (*e.g.*, *id.* ¶¶ 2-3), and broadly accuse defendants of an "invasion into Plaintiffs' zone of privacy" (*id.* ¶ 304), they never claim the kind of emotional distress or reputational damage that potentially flows from a true invasion of privacy. Instead, they allege only economic harm based on "[t]he cash value of [their] medical information" in the advertising market. *Id.* ¶¶ 53-57, 304.

This Court rejected that very theory in *Facebook Internet*. There, as here, the plaintiffs claimed "that the information collected by Facebook's cookies ha[d] economic value" and that this "value may be significant when user information is aggregated." 140 F. Supp. 3d at 931. But they did *not* allege that "anyone was willing to pay for their personal information or that [Facebook's] purported conduct lessened the value of that information or affected its marketability." *Id.* at 930. Because the plaintiffs had not claimed "that they personally *lost* the opportunity to sell their information or that the value of their information was somehow *diminished* after it was collected by Facebook," this Court held that they had failed to establish the necessary injury in fact. *Id.* at 931-32 (emphases added). And it noted that many other

"courts have found insufficient for standing purposes generalized assertions of economic harm based solely on the alleged value of personal information." *Id.* at 930.[5]

Plaintiffs halfheartedly attempt to distinguish these authorities by alleging that *medical* information is especially valuable to advertisers. Compl. ¶ 57. But even accepting this allegation as true, and even assuming that plaintiffs' information can truly be deemed "medical" in nature (*but see* pp. 28-30 *infra*), plaintiffs have failed to allege a *diminution* in its value; they have failed to "connect th[e] value [of their information] to a realistic economic harm or loss that is attributable to [defendants'] alleged conduct." *Facebook Internet*, 140 F. Supp. 3d at 931. As in *Facebook Internet*, they have not alleged (1) that they have the ability to sell their alleged information to unspecified third-party buyers; (2) that they would actually choose to do so; or (3) that those buyers would now pay less for this information than they would have absent defendants' alleged conduct. *See id.* at 930.

Indeed, in a post-*Spokeo* case against a hospital, where the plaintiff *did* allege that "the value of her personally identifiable information [was] diminished" when hackers obtained her actual *medical information and Social Security number*, the court dismissed the case for lack of standing because the plaintiff had failed to "explain *how* the hackers' possession of that information ha[d] diminished its value" or "assert that she would ever actually sell her own personal information." *Khan v. Children's Nat'l Health Sys.*, 2016 WL 2946165, at *6 (D. Md.

[5] *See, e.g.*, *In re Zappos.com Inc.*, 108 F. Supp. 3d 949, 954 (D. Nev. 2015) (no standing because "Plaintiffs do not allege any facts explaining how their personal information became less valuable . . . or that they attempted to sell their information and were rebuffed"); *In re Google, Inc. Privacy Policy Litig.*, 2013 WL 6248499, at *5 (N.D. Cal. Dec. 3, 2013) ("[I]njury-in-fact . . . requires more than an allegation that a defendant profited from a plaintiff's personal identification information. Rather, a plaintiff must allege how the defendant's use of the information deprived the plaintiff of the information's economic value."); *Low v. LinkedIn Corp.*, 2011 WL 5509848, at *1-2, *5 (N.D. Cal. Nov. 11, 2011) (no standing in case alleging economic loss from LinkedIn's transmission of plaintiff's personal information to third parties, because plaintiff failed to explain "how he was deprived of the economic value of [his] personal information simply because [it] was purportedly collected by a third party" (internal quotation marks omitted)); *LaCourt v. Specific Media, Inc.*, 2011 WL 1661532, at *5 (C.D. Cal. Apr. 28, 2011) (no standing in case alleging that defendant used plaintiffs' personal information for targeted advertising, because plaintiffs had not referenced "a single individual who was foreclosed from entering into a 'value-for-value exchange' as a result of [defendant's] conduct").

May 19, 2016) (emphasis added); *see also Gubala v. Time Warner Cable, Inc.*, 2016 WL 3390415, at *4 (E.D. Wis. June 17, 2016) (no standing based on defendant's retention of plaintiff's "personally identifiable information"; "[a] statement that consumers highly value the privacy of their personally identifiable information . . . does not demonstrate that the plaintiff has suffered a concrete injury"); *cf. In re Nickelodeon Consumer Privacy Litig.*, __ F.3d __, 2016 WL 3513782, at *6-8 (3d Cir. June 27, 2016) (finding Article III standing based on the alleged disclosure of minors' private, personal information). Plaintiffs here allege far less.

In sum, plaintiffs have failed to establish standing as to any of the defendants for the exact reasons outlined in *Facebook Internet*: They have not alleged that defendants' conduct resulted in concrete harm. 140 F. Supp. 3d at 932. After *Spokeo*, there is no longer any reason to treat plaintiffs' statutory claims any differently from their common-law claims; they all fall far short of alleging concrete harm, and the Court lacks jurisdiction over each of them.[6]

## II. THE CLAIMS AGAINST THE HEALTHCARE DEFENDANTS SHOULD BE DISMISSED UNDER RULE 12(b)(2).

### A. This Court Lacks Personal Jurisdiction over the Healthcare Defendants.

Plaintiffs assert that the Court may exercise personal jurisdiction over the healthcare defendants even though they are not California residents because they "operate and market their

[6] In addition to their failure to allege a "concrete" harm against all defendants, plaintiffs also fail to allege a "particularized" harm against BJC and Cleveland Clinic. "For an injury to be 'particularized,' it 'must affect the plaintiff in a personal and individual way.'" *Spokeo*, 136 S. Ct. at 1548; *see also, e.g., Allen v. Wright*, 468 U.S. 737, 755-56 (1984) (dismissing racial discrimination claim where plaintiffs failed to allege that they were personally subject to the challenged discrimination or were personally denied equal treatment); *Warth v. Seldin*, 422 U.S. 490, 504 (1975) (dismissing housing discrimination claim where plaintiffs failed to allege a personal interest in the subject property or a personal denial of equal treatment). Jane Doe II does not allege to have communicated any "personal" information to BarnesJewish.org or ClevelandClinic.org. *See* Compl. ¶¶ 175-77, 188. She alleges only that Facebook received copies of the public URLs for the webpages she was browsing *on behalf of someone else*. Plaintiffs' failure to allege that Facebook received any personal information communicated to BJC and Cleveland Clinic further precludes Article III jurisdiction as to those two defendants. *See Warth*, 422 U.S. at 502-07.

websites throughout the country and this district." Compl. ¶ 17. This allegation cannot establish either general or specific personal jurisdiction over any of the healthcare defendants.[7]

The test for general jurisdiction is whether a corporation's "affiliations with the State are so 'continuous and systematic' as to render [it] essentially at home in the forum State." *Daimler AG v. Bauman*, 134 S. Ct. 746, 755-56, 760 (2014). Plaintiffs do not contend that any of the healthcare defendants has any meaningful presence in California at all, and operating a website, by itself, plainly does not "signal a non-resident defendant's intent to 'sit down and make itself at home' in the forum." *Mavrix Photo, Inc. v. Brand Tech, Inc.*, 647 F.3d 1218, 1223 (9th Cir. 2011).

The elements required for specific jurisdiction are that (1) the non-resident purposefully directed its activities to the forum or purposefully availed itself of the privilege of conducting activities in the forum; (2) the plaintiff's claims arise out of the defendant's forum-related conduct; and (3) any exercise of jurisdiction over the non-resident defendant would comport with fair play and substantial justice—*i.e.*, it must be reasonable. *Schwarzenegger v. Fred Martin Motor Co.*, 374 F.3d 797, 800 (9th Cir. 2004).

Plaintiffs' allegations do not satisfy either of the first two elements, on which they bear the burden, so it is unnecessary to consider the third. With respect to the first element, plaintiffs have not alleged any facts indicating that any of the healthcare defendants specifically directed their website activities to California residents. "If the defendant merely operates a website, even a highly interactive website, that is accessible from, but does not target, the forum state, then the defendant may not be haled into court in that state without offending the Constitution." *DFSB Kollective Co. v. Bourne*, 897 F. Supp. 2d 871, 881 (N.D. Cal. 2012) (applying the three-part test outlined in *Calder v. Jones*, 465 U.S. 783 (1984), to evaluate purposeful direction); *see also Cybersell, Inc. v. Cybersell, Inc.*, 130 F.3d 414, 419 (9th Cir. 1997) (operation of website accessible in Arizona did not give rise to jurisdiction where defendant entered into no contracts

[7] Personal jurisdiction is improper as to defendant ACS because ACS's Terms of Service contain a clause requiring exclusive jurisdiction in the State of Georgia.

in, made no sales in, received no telephone calls from, earned no income from, and sent no messages to Arizona).

As for the second element, the healthcare defendants' operation of their websites occurred entirely outside of California, as did the alleged effects of that activity. Indeed, each of the plaintiffs resides outside California, two in Missouri and one in Kansas. Compl. ¶¶ 6-8. Consequently, even if any plausible harm had been caused by the healthcare defendants' alleged conduct, it would have been felt in Missouri or Kansas, not in California. *See Schwarzenegger*, 374 F.3d at 802. Plaintiffs have therefore failed to satisfy the test for specific jurisdiction.

**B. The Eleventh Amendment Bars Jurisdiction over MD Anderson.**

Plaintiffs' claims against MD Anderson are also barred by the Eleventh Amendment, which "prohibit[s] federal courts from hearing suits brought by private citizens against state governments without the state's consent." *Sofamor Danek Grp., Inc. v. Brown*, 124 F.3d 1179, 1183 (9th Cir. 1997). As set forth in MD Anderson's contemporaneously filed Request for Judicial Notice, MD Anderson is a Texas State agency whose Eleventh Amendment immunity may be abrogated only by an act of Congress or a waiver by the Texas State Legislature. *See Pennhurst State Sch. & Hosp. v. Halderman*, 465 U.S. 89, 99-100 (1984). Neither Congress nor Texas has waived MD Anderson's Eleventh Amendment immunity for plaintiffs' California state-law claims. And plaintiffs' only federal claim against MD Anderson is for alleged violations of the Wiretap Act, which does not permit suit against MD Anderson because it is not a "person" under the Act. 18 U.S.C. § 2520(a); *see Seitz v. City of Elgin*, 719 F.3d 654, 656-57 (7th Cir. 2013) ("Only a 'person' can violate § 2511(1)."); Compl. ¶¶ 40-52, 265; *cf. Vt. Agency of Nat. Res. v. U.S. ex rel. Stevens*, 529 U.S. 765, 779 (2000) (holding that False Claims Act does not subject a state to liability because a state is not a "person" under the Act).

## III. THE COMPLAINT SHOULD BE DISMISSED AS TO ALL DEFENDANTS UNDER RULE 12(b)(6).

As a threshold matter, all of plaintiffs' claims are barred because plaintiffs consented to Facebook's receipt and use of their information. But even if the claims were not barred by

plaintiffs' consent, the complaint still should be dismissed in its entirety because plaintiffs failed to plead the necessary elements of each claim they assert.

### A. All of Plaintiffs' Claims Fail Because They Consented to the Collection and Use of Information About Their Visits to Defendants' Websites.

The absence of consent is either an express or implicit component of each of plaintiffs' claims.[8] "There may be subtle differences" among the consent doctrines, but "the question under [each] is essentially the same: Would a reasonable user who viewed [the defendants'] disclosures have understood that [Facebook] was collecting [the information at issue]?" *Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1190, 1212 (N.D. Cal. 2014). If so, plaintiffs cannot recover against any of the defendants. *See* RESTATEMENT (SECOND) OF TORTS § 892A (1979) ("One who effectively consents to conduct of another intended to invade his interests cannot recover in an action of tort for the conduct."). Plaintiffs' consent to Facebook's policies independently bars their claims.

Plaintiffs acknowledge (Compl. ¶ 59) that when they signed up for and used Facebook, they agreed to Facebook's SRR, Data Policy, and Cookie Policy, which disclose that Facebook: (1) "work[s] with third-party companies who . . . use advertising or related products"; (2) "collect[s] information when you visit or use third-party websites," including "information about the websites"; (3) "use[s] *all* of the information we have about you to show you relevant ads"; (4) "provide[s] [third parties] with information about the reach and effectiveness of their

[8] *See, e.g.*, 18 U.S.C. § 2511(2)(d) (no liability under the Wiretap Act where "one of the parties to the communication has given prior consent"); *Hill v. Nat'l Coll. Athletic Ass'n*, 7 Cal. 4th 1, 26 (1994) ("The maxim of the law 'volenti non fit injuria' (no wrong is done to one who consents) applies as well to the invasion of privacy tort."); Cal. Penal Code §§ 631(a), 632(a) (CIPA claim requires interception of covered information "without the consent of all parties" to the communication); *Evan F. v. Hughson United Methodist Church*, 8 Cal. App. 4th 828, 834 (1992) (negligence action requires that the defendant took on a legal duty toward the plaintiff and breached that duty); *Guz v. Bechtel Nat'l Inc.*, 24 Cal. 4th 317, 349 (2000) (claim for breach of covenant of good faith and fair dealing requires allegation that contracting party "unfairly frustrat[ed] the other party's right to receive the benefits of the agreement actually made"); *S. Tahoe Gas Co. v. Hofman Land Improvement Co.*, 25 Cal. App. 3d 750, 765 (1972) (to prove fraud claim, plaintiff must demonstrate that defendant made a false statement or suppressed a material fact (here, in Facebook's disclosures)).

advertising"; (5) uses "[c]ookies" to "deliver ads," "make them more relevant to you," and "show you . . . ad[s] based on the websites you visit or the apps you use—*all across the Internet and mobile ecosystem*"; and (6) permits people to "control" these processes or opt out of targeted advertising. *Id.* Ex. B at 2-3, 5-6, Ex. C at 2, 4 (emphases added).

Plaintiffs assert that their consent to these policies is irrelevant because Facebook did not disclose that it collects "*medical* information and communications" specifically. *Id.* ¶ 65 (emphasis added). Putting aside, once again, whether this is actually "medical information," Facebook's disclosures could not be clearer: Facebook collects information about its users' browsing histories "*all* across the Internet and mobile ecosystem," and "use[s] *all* of the information we have about you to show you relevant ads." *Id.* Ex. B at 5, Ex. C at 2 (emphases added). "A contractual term is not ambiguous" or incomplete "just because it is broad." *F.B.T. Prods., LLC v. Aftermath Records*, 621 F.3d 958, 964 (9th Cir. 2010). And disclosures about data collection cannot be "slice[d] . . . too thin"; if a reasonable user would understand that the alleged conduct was covered, that is enough. *Perkins*, 53 F. Supp. 3d at 1215.

Because it is impossible for a service to list every conceivable form of information that it collects from third-party websites, courts have routinely dismissed claims based on the collection of information where the defendants' terms of service were far more generalized than Facebook's. *See, e.g.*, *Perkins*, 53 F. Supp. 3d at 1195, 1212 (dismissing claim that LinkedIn harvested non-user email addresses from plaintiffs' contact lists for marketing purposes because users were notified that LinkedIn was "asking for *some* information from" the email account and were then given a choice of forbidding this collection (emphasis added)); *Del Vecchio v. Amazon.com, Inc.*, 2012 WL 1997697, at *6 (W.D. Wash. June 1, 2012) (dismissing cookie-tracking claim involving financial information and mailing addresses because Amazon's terms of use "notif[ied] visitors that [Amazon] will . . . place . . . cookies on their computers and use those cookies to monitor and collect information," even though terms did not say anything specific about what kind of information would be obtained); *Mortensen v. Bresnan Commc'n, LLC*, 2010 WL 5140454, at *4-5 (D. Mont. Dec. 13, 2010) (terms of service barred cookie-tracking claim even though defendant "did not fully describe its intent to funnel [the]

customer's complete, unfiltered Internet traffic to a third-party processor for profiling and ad-serving"; it was sufficient for defendant to disclose "that Plaintiffs' *electronic transmissions* would be monitored and would in fact be transferred to third-parties for the purposes of providing '*content or services*'" (emphases added)).

Facebook's disclosures, standing alone, were more than adequate to put plaintiffs on notice of all of the conduct alleged in the complaint, and to bar all of their claims. But it is worth noting that the disclosures on the healthcare defendants' sites made the same points. First, these policies explained that third parties would use cookies to collect information about users' browsing on their sites. *See* p. 8 *supra*. Second, they specifically directed users to consult the privacy policies of the third-party sites for information about data collection. *See, e.g.*, Compl. Ex. F at 5 ("read the privacy policies of each site you visit to determine what information that site may be collecting about you"); *id.* Ex. G. §§ 4, 13 ("review the privacy policies of other sites carefully"). Plaintiffs' claims are all barred.

**B. The Complaint Fails to Allege the Specific Elements of Each Claim.**

**1. Plaintiffs Fail to State a Claim under the Wiretap Act.**

Plaintiffs claim that Facebook violated the Wiretap Act by intercepting the contents of their communications with the healthcare defendants' sites, and that the healthcare defendants violated the Act by somehow "facilitat[ing]" that alleged violation. *Id.* ¶¶ 254-56, 265. The Wiretap Act provides a right of action against anyone who (1) "intercepts" the (2) "contents" of a "wire, oral, or electronic communication" using (3) a "device." 18 U.S.C. §§ 2510, 2511(1), 2520. Plaintiffs have alleged none of these three elements against any of the defendants.[9]

***Interception***. A communication cannot be "intercepted" by one of its parties, because a party is the *direct recipient* of the communication. *See, e.g.*, *Marsh v. Zaazoom Sols., LLC*, 2012 WL 952226, at *17 (N.D. Cal. Mar. 20, 2012) ("[A]n 'interception' as defined under the [Wiretap] Act could not exist where the plaintiff himself transmitted the information to [the

[9] The Wiretap Act claim fails against the healthcare defendants for the additional reason that it requires "intentional" conduct, 18 U.S.C. § 2511(1)(a), and plaintiffs disclaim any allegation that the healthcare defendants acted with intent. *See* Compl. ¶¶ 290, 317.

defendant] which was the second party to the communication." (internal quotation marks omitted)).[10] Thus, the Wiretap Act expressly provides that "[i]t shall not be unlawful . . . for a person . . . to intercept a wire, oral or electronic communication where such person is a party to the communication." 18 U.S.C. § 2511(2)(d). This exemption is fundamental to the Act, which prohibits *wiretapping*, not receiving information.

According to the complaint, when plaintiffs visited the healthcare defendants' sites, their browsers sent two *separate* communications: (1) a GET request to the healthcare site requesting that information be displayed on the browser; and (2) a separate GET request to Facebook accompanied by a referer header with the URL of the webpage on which Facebook content was being loaded. Compl. ¶¶ 32, 50-51; pp. 3-4 *supra*. The healthcare defendants received only the first communication, to which they were parties: Plaintiffs repeatedly allege that the named plaintiffs deliberately and directly communicated the GET requests to those defendants' websites. *See, e.g.*, Compl. ¶¶ 117, 175, 319, 325. And Facebook received only the second communication, to which *it* was a party: Plaintiffs allege that the referer header was sent *directly* from "the user's web-browser . . . to *Facebook's server*." *Id.* ¶ 50(f) (emphasis added).

In other words, as plaintiffs themselves allege, "Facebook's acquisition of the plaintiff's communications to and from the medical websites was accomplished through a *separate channel* than the path of the *actual* communication between the users and the medical websites." *Id.* ¶ 255 (emphases added). This concession is dispositive both of plaintiffs' claim that Facebook "wiretapped" them and that the healthcare defendants "facilitated" this wiretapping. Each of the defendants was plainly a party to the communications that it received from plaintiffs' browsers. *See In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 142-43 (3d Cir. 2015) ("*Google Cookie Placement*") (dismissing a substantively identical Wiretap Act claim because the defendants were parties to the communications; they had "acquired the plaintiffs' internet history information by way of *GET requests that the plaintiffs sent directly to the*

[10] *See also Crowley v. CyberSource Corp.*, 166 F. Supp. 2d 1263, 1269 (N.D. Cal. 2001) (because "Amazon merely received the information transferred to it by [plaintiff]," it "acted as no more than the second party to a communication"; "[t]his is not an interception"); *cf. Bartnicki v. Vopper*, 532 U.S. 514, 523 (2001); *United States v. Reed*, 575 F.3d 900, 916 (9th Cir. 2009).

*defendants*," and an "intended recipient of a communication is necessarily one of its parties" (emphasis added)).

Plaintiffs make two feeble attempts to circumvent this problem. First, they allege that they "ha[d] no reason to suspect that Facebook acquired the communications." Compl. ¶ 267. That is both groundless and irrelevant. Both Facebook and the healthcare defendants informed plaintiffs of precisely that fact. *See* pp 5-8, 16-18 *supra*. And plaintiffs' awareness (or lack of awareness) of their own browsers' communications with Facebook has no bearing on whether Facebook was a party to those communications. Because the Wiretap Act "is, after all, a *wiretapping* statute," "a deceit upon the sender" does not "affect[] the presumptive non-liability of parties." *Google Cookie Placement*, 806 F.3d at 143; *see also Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878-79 (9th Cir. 2002) (no interception where employer covertly obtained access to employee's website using another employee's password because information was not obtained during transmission); *Bunnell v. Motion Picture Ass'n of Am.*, 567 F. Supp. 2d 1148, 1153 (C.D. Cal. 2007) (no interception where defendant configured plaintiffs' email software to simultaneously forward exact copies of emails to defendant). If a third-party server were deemed to "intercept" a referer header every time the user was unaware that his browser sent it, the vast majority of web-content providers would be in perpetual violation of the Wiretap Act.

Second, plaintiffs claim that "Facebook's acquisition of the information was contemporaneous to the sending and receipt of [the] communications." Compl. ¶ 254. But the timing does not change the key fact here: that plaintiffs' own browsers sent Facebook the referer header information directly. *See Bunnell*, 567 F. Supp. 2d at 1153-54 (whether defendant "received the forwarded messages in milliseconds or days . . . ma[de] no difference"; they were not "intercepted" because they were sent by separate copy); *see also Konop*, 302 F.3d at 878.

***Content***. The Wiretap Act applies only to the "contents" of a communication—*i.e.*, "any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8). The referer headers allegedly acquired here do not fall within the statutory definition. In *Facebook Internet*, this Court held that a referer header sent to Facebook by a user's browser does not qualify as "content" because it is nothing more than "record information regarding the

characteristics of the message that is generated in the course of the communication.'" 140 F. Supp. 3d at 935 (quoting *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1106-07 (9th Cir. 2014)). The Court emphasized that "Plaintiffs may never be able to state [a] Wiretap Act claim, particularly since their arguments on this issue are so unpersuasive." *Id.* at 935-36.

Plaintiffs nonetheless allege that the referer URLs their browsers sent to Facebook are content because they include the "search queries which Plaintiffs sent to the medical websites." Compl. ¶¶ 50(f), 256. Not so. By definition, a URL does not convey the "meaning" of the communication with the host server; it simply identifies the *location* of the requested webpage on the Internet. *Zynga* expressly contemplated that a referer header could disclose that a person viewed the "page of a gay support group," but it still held that such URLs "function[] like an 'address,'" not content. 750 F.3d at 1107. That decision is binding in this case, just as it was in *Facebook Internet*.[11]

***Device***. Plaintiffs also fail to sufficiently allege the use of an "electronic, mechanical, or other device." 18 U.S.C. § 2510(4). The complaint offers a bare list of items that it claims to be "devices": (a) "cookies . . . used to track the Plaintiffs' communications"; (b) "Plaintiffs' web-browsers"; (c) "Plaintiffs' computing devices"; (d) "Facebook's web-servers"; (e) "[t]he web-servers of the medical websites"; (f) "computer code deployed by Facebook"; and even (g) "[t]he plan Facebook carried out to effectuate the tracking and interception of user communications." Compl. ¶ 261. But none of these items "can be used to intercept" plaintiffs' communications with the healthcare defendants, as required under the statutory definition of "device." 18 U.S.C. § 2510(5). A cookie is a "small text file[]" that stores information (Compl. ¶ 41); it cannot intercept anything. Neither a browser, nor a server, nor code is a "device." *See, e.g.*, *Crowley v. CyberSource Corp.*, 166 F. Supp. 2d 1263, 1269 (N.D. Cal. 2001) ("drive or server on which the e-mail was received" not a device under Wiretap Act); *Potter v. Havlicek*, 2008 WL 2556723, at *8 (S.D. Ohio June 23, 2008) ("the word 'device' does not encompass

[11] In *Google Cookie Placement*, the Third Circuit suggested in *dicta* that certain referer headers might qualify as content if they include specific information that the browser has requested. 806 F.3d at 136-39. But the court dismissed the case under the Wiretap Act's "party" exception and did not reach this question. *Id.* at 139-40.

software"; it is a "piece of equipment or a mechanism designed to serve a special purpose or perform a special function"). And if a "plan" could qualify as a device, the statutory requirement would be meaningless.

**2. Plaintiffs Fail to State a Claim under CIPA.**

Plaintiffs assert claims under two provisions of CIPA: Sections 631 and 632. *See* Compl. ¶¶ 305-21. Both are deficient under California law, preempted by the Wiretap Act, and separately inapplicable against the healthcare defendants because they are foreign entities.

***Section 631(a).*** Like the Wiretap Act, CIPA "prohibits the interception of wire communications and disclosure of the contents of such intercepted communications." *Tavernetti v. Super. Ct.*, 22 Cal. 3d 187, 190 (1978) (emphases added). "Section 631 was aimed at one aspect of the privacy problem—eavesdropping, or the secret monitoring of conversations by third parties." *Ribas v. Clark*, 38 Cal. 3d 355, 359 (1985); *see Google Cookie Placement*, 806 F.3d at 152 (same). This claim fails as to all defendants for each of three independent reasons.[12]

First, as with the federal wiretap claim, plaintiffs do not allege any "eavesdropping," because their own allegations establish that defendants were parties to the communications at issue. *See* pp. 18-20 *supra*; *Warden v. Kahn*, 99 Cal. App. 3d 805, 811 (1979) ("[S]ection 631 . . . has been held to apply only to eavesdropping by a third party and not to recording by a participant to the conversation.").[13] Second, as explained in *Facebook Internet*, plaintiffs have not alleged that Facebook acquired "the contents or meaning of any message." 140 F. Supp. 3d

[12] In addition, as with the federal wiretap claim discussed above, plaintiffs' CIPA claim fails against the healthcare defendants because it requires "intentional" conduct, *see* Cal. Pen. Code § 631(a), and plaintiffs disclaim any allegation that the healthcare defendants acted with intent. *See* Compl. ¶¶ 290, 317.

[13] In *Facebook Internet*, the Court declined to dismiss the plaintiffs' Section 631 claim on this ground because the plaintiffs "allege[d] that they were unaware that Facebook was surreptitiously tracking them after they logged out of the Facebook website." 140 F. Supp. 3d at 936. Here, the complaint makes clear that plaintiffs *were* aware of Facebook's collection of data. *See* pp. 5-8, 16-18 *supra*. And in any event, Facebook's status as a party does not depend on such awareness. *See Google Cookie Placement*, 806 F.3d at 152 (district court correctly "dismissed the [plaintiffs'] § 631(a) claim for the same reasons that it dismissed the plaintiffs' wiretapping claim": because "Google was itself a party to all the electronic transmissions," and regardless of whether plaintiffs had been deceived).

at 936; *see* Cal. Penal Code § 631(a). Third, plaintiffs have not attempted to allege that Facebook acquired their communications using "a machine, instrument, or contrivance." Cal. Penal Code § 631(a). A cookie is "a small text file containing a limited amount of information which sits idly on a user's computer until contacted by a server"; it does not "fall into [any] of [CIPA's] three categories." *Facebook Internet*, 140 F. Supp. 3d at 937.

***Section 632(a).*** Plaintiffs' separate CIPA claim against Facebook alone[14] must also be dismissed. Section 632(a) creates an action against "[e]very person who, intentionally and without the consent of all parties to a confidential communication, by means of any electronic amplifying or recording device, . . . records the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device, except a radio." Cal. Penal Code § 632(a). Once again, plaintiffs have failed to allege any of the elements of this claim.

First, plaintiffs here *did* consent. *See* pp. 5-8, 16-18 *supra*. Second, plaintiffs' communications were in no way "confidential"; they were transmitted automatically by plaintiffs' own browsers when they visited the healthcare sites. "Decisions from the California appellate courts . . . suggest that internet-based communications cannot be confidential" because they are easily recorded and shared. *In re Google Inc. Gmail Litig.*, 2013 WL 5423918, at *22 (N.D. Cal. Sept. 26, 2013).[15] Third, plaintiffs have not alleged that Facebook used an "electronic amplifying or recording device." Indeed, the statute's specific reference to "a telegraph, telephone, or other device, except a radio," demonstrates that it was intended to apply to traditional recording mechanisms, not idle text files like cookies.

---

[14] The heading of plaintiffs' CIPA cause of action suggests that it is asserted "[a]gainst [a]ll [d]efendants" (Compl. p. 71), but the paragraph devoted to Section 632 mentions only Facebook (*id.* ¶ 320), and any claim based on the alleged "recording" of a communication cannot logically apply to the healthcare defendants under these circumstances.

[15] *See, e.g.*, *People v. Nakai*, 183 Cal. App. 4th 499, 518 (2010) (defendant's instant messages not confidential, even though he intended that they be kept between him and recipient, because they "could have easily been shared or viewed by . . . any computer user with whom [the recipient] wanted to share the communication"); *People v. Griffitt*, 2010 WL 5006815, at *6 (Cal. Ct. App. Dec. 9, 2010) (rejecting Section 632 claim because "[e]veryone who uses a computer knows that the recipient of e-mails and participants in chat rooms can . . . share them with whoever they please, forward them or otherwise send them to others.").

***Preemption***. Plaintiffs' CIPA claim—along with all of their other state-law claims—is preempted by the Wiretap Act, which provides that "[t]he remedies and sanctions described in this chapter with respect to the *interception of electronic communications* are the *only judicial remedies* and sanctions for nonconstitutional violations of this chapter involving such communications." 18 U.S.C. § 2518(10)(c) (emphases added). This provision works an "express preemption" of state-law claims based on the alleged interception of electronic communications. *Bunnell*, 567 F. Supp. 2d at 1154; *see also Quon v. Arch Wireless Operating Co.*, 445 F. Supp. 2d 1116, 1138 (C.D. Cal. 2006), *aff'd in part, rev'd in part on other grounds*, 529 F.3d 892 (9th Cir. 2008). And each of plaintiffs' state-law claims is based on an alleged interception of electronic communications, including their CIPA claim. *See, e.g.*, Compl. ¶¶ 295, 315, 329.

The Wiretap Act also impliedly preempts such claims because it "leaves no room in which the states may further regulate." *In re Google Inc. Street View Elec. Commc'ns Litig.*, 794 F. Supp. 2d 1067, 1084-85 (N.D. Cal. 2011). The statute was enacted

> to provide legal certainty to users and developers of innovative communications technologies with bright line rules for liability. In so regulating, Congress struck a balance between the right to the privacy of one's electronic communications against the ability of users to access communications technologies without fear of liability for inadvertent interception. State regulation acting in addition . . . might serve to obscure the legislative scheme surrounding innovative communications technologies that Congress intended to clarify through the Act, or could serve to upset the fragile balance considered by Congress.

*Id.* at 1085; *see also Bunnell*, 567 F. Supp. 2d at 1154 (similar); *Quon*, 445 F. Supp. 2d at 1138.

This case demonstrates exactly why that objective is so important. Plaintiffs have brought *nine* different state-law claims based on allegations that are substantively identical to their Wiretap Act claim. If Internet service providers were subject to liability for routine receipt and use of data and marketing activities based on any or all of these theories, the requirements carefully set forth in the Wiretap Act would have little meaning, with devastating effects on innovation.[16]

[16] Defendants recognize that there is a split in authority on both express and implied preemption. One court has concluded that "the plain language of § 2518(10)(c) simply states

***Extra-territoriality.*** Plaintiffs' CIPA claims must be dismissed as to the healthcare defendants for the additional reason that they are all located outside of California. "[A] presumption exists against the extraterritorial application [of California] state law." *O'Connor v. Uber Techs., Inc.*, 58 F. Supp. 3d 989, 1004 (N.D. Cal. 2014) (citing *Sullivan v. Oracle Corp.*, 51 Cal. 4th 1191 (2011)); *Norwest Mortg., Inc. v. Super. Ct.*, 72 Cal. App. 4th 214, 222-25 (1999) ("We ordinarily presume the Legislature did not intend the statutes of this state to have force or operation beyond the boundaries of the state."). This presumption is overcome only if extraterritorial "intention is clearly expressed or reasonably to be inferred from the language of the act or from its purpose, subject matter or history." *Sullivan*, 51 Cal. 4th at 207 (internal quotation marks omitted). Nothing in CIPA expresses an intention for the Act to apply to an alleged out-of-state interception by a non-California defendant of a non-California plaintiff's communications.

### 3. Plaintiffs Fail to State a Claim for Intrusion Upon Seclusion or California Constitutional Invasion of Privacy.

Plaintiffs' two other privacy-related claims (Compl. ¶¶ 295-304, 322-31) have similar elements and are commonly considered in tandem. *See Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 287 (2009).[17] "First the defendant must intentionally intrude into a place, conversation, or

---

that a violation of the chapter has limited remedies and sanctions," which "does not mean that violations of *other* laws (such as the CIPA) cannot provide for *other* remedies and sanctions." *Shively v. Carrier IQ, Inc.*, 2012 WL 3026553, at *3 (N.D. Cal. July 24, 2012). This reading would render Section 2518(10)(c) meaningless: Because Congress specifically delineated the sanctions and remedies that result from a violation of the Wiretap Act, *see* 18 U.S.C. §§ 2511(4), 2520(b), there was no need to add a provision making the obvious point that no additional relief and sanctions are available for a claim *under that very statute*. Courts have also rejected arguments on implied preemption based largely on legislative history suggesting that the Wiretap Act was "an attempt to establish minimum standards" rather than occupy the field. *Shively*, 2012 WL 3026553, at *6-7; *see also Leong v. Carrier IQ Inc.*, 2012 WL 1463313, at *3 (C.D. Cal. Apr. 27, 2012); *Valentine v. NebuAd*, 804 F. Supp. 2d 1022, 1029 (N.D. Cal. 2011). These cases, however, largely ignore both (1) the comprehensive nature of the Wiretap Act and (2) its objective of providing certainty and striking a balance between privacy rights and free access to communications technologies.

[17] As with plaintiffs' CIPA claim, California's common law and constitutional intrusion laws do not apply to the healthcare defendants because the alleged violations involved conduct that took place outside California and allegedly affected residents of other states. *See* p. 25

matter as to which the plaintiff has a reasonable expectation of privacy," meaning that "the defendant . . . penetrated some zone of physical or sensory privacy or obtained access to data by electronic or other covert means, in violation of the law or social norms." *Id.* at 286 (internal quotation marks omitted). "Second, the intrusion must occur in a manner highly offensive to a reasonable person." *Id.* "The gravamen" of the claim "is the mental anguish sustained when both conditions of liability exist." *Id.* Neither element exists here.[18]

***Reasonable expectation of privacy.*** Plaintiffs "could not have held a subjective expectation of privacy in their browsing histories that was objectively reasonable, because 'Internet users have no expectation of privacy in [the identities of] . . . the websites they visit.'" *Facebook Internet*, 140 F. Supp. 3d at 933 n.5 (quoting *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2007)). At least when it comes to the location of those sites, "[p]laintiffs 'should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information.'" *Id.* (quoting *Forrester*, 512 F.3d at 510). Moreover, plaintiffs failed to take the available measures to safeguard their information. *See Med. Lab. Mgmt. Consultants v. ABC, Inc.*, 306 F.3d 806, 813 (9th Cir. 2002). They indisputably had the opportunity to "manage the content and information [they] share[d] when [they] use[d] Facebook" (Compl. Ex. B at 6), but they do not allege that they took any actions to prevent Facebook from using referer header information for purposes of targeted advertising.

***Highly offensive manner.*** Nor did any of the defendants *use* plaintiffs' information "in a manner highly offensive to a reasonable person." *Hernandez*, 47 Cal. 4th at 286. This demanding element requires "an exceptional kind of prying into another's private affairs," such as "taking the photograph of a woman in the hospital with a 'rare disease that arouses public

---

*supra*; *e.g.*, *Hill*, 7 Cal. 4th at 17 (California voters enacted a constitutional right of privacy only to "create[] a legal and enforceable right of privacy *for every Californian*" (emphasis added)).

[18] In addition to the deficiencies discussed below, plaintiffs also fail on two grounds to allege that the healthcare defendants "intentionally intruded" into a private matter. First, plaintiffs allege that they intended for the healthcare defendants to receive their communications. *See, e.g.*, Compl. ¶ 259. Second, plaintiffs repeatedly admit that they lack any facts showing that the healthcare defendants knowingly or intentionally disclosed communications to Facebook. *See, e.g.*, *id.* ¶¶ 290, 317.

curiosity'" or "using a telescope to look into someone's upstairs bedroom window for two weeks and taking 'intimate pictures' with a telescopic lens." *Med. Lab.*, 306 F.3d at 819. And naturally, conduct motivated by "legitimate business reasons"—as opposed to "socially repugnant . . . reasons"—cannot be considered "highly offensive to a reasonable person." *Hernandez*, 47 Cal. 4th at 286, 297; *see also Fogelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986, 992 (2011) (dismissing as "routine commercial behavior" the unauthorized procurement of plaintiff's home address in order to mail him coupons and other advertisements).

The routine marketing activities and public education functions described in the complaint fall far short of these standards. Plaintiffs do not allege "the absence of any reasonable justification or beneficial motivation," *Hernandez*, 47 Cal. 4th at 297; rather, they claim that Facebook uses their information for the exact reason disclosed in its Data Policy: "to improve our advertising and measurement systems so we can show you relevant ads." Compl. Ex. B at 3. Courts in this Circuit consistently reject privacy claims based on such conduct. *See, e.g.*, *In re Google, Inc. Privacy Policy Litigation*, 58 F. Supp. 3d 968, 985 (N.D. Cal. 2014) ("Courts in this district have consistently refused to characterize the disclosure of common, basic digital information to third parties as serious or egregious violations of social norms."); *In re iPhone App. Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) (no privacy claim where defendant released plaintiffs' "unique device identifier number, personal data, and geolocation information" from cell phones to third parties without their "knowledge and consent"); *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012) (no privacy claim where LinkedIn allegedly disclosed user browsing history to third parties; "[e]ven disclosure of personal information, including social security numbers, does not constitute an 'egregious breach of social norms' [sufficient] to establish an invasion of privacy" (internal quotation marks omitted)).

The cases that have upheld privacy claims based on disclosures of medical information make it even clearer that plaintiffs' claims fall far short of the mark. Some involved the *in-person* recording of medical *treatment* in the immediate aftermath of a traumatic event.[19]

[19] *See, e.g.*, *Schulman v. Grp. W Prods., Inc.*, 18 Cal. 4th 200, 209 (1998) (following car accident, cameraman "filmed plaintiffs' extrication from the car, the flight nurse and medic's

Others involved the collection and use of official health *records* from medical treatment facilities for wildly inappropriate purposes—for example, "to intimidate, embarrass and humiliate" a victim of sexual battery during a cross-examination in the batterer's criminal trial. *Susan S. v. Israels*, 55 Cal. App. 4th 1290, 1298 (1997).[20] This case does not resemble these facts.

**4. Plaintiffs Have Not Asserted a Claim for "Negligence Per Se"**

Plaintiffs bring a claim styled "negligence per se" based on defendants' alleged violation of "several criminal and civil laws," including two healthcare-related statutes: the Health Insurance Portability and Accountability Act ("HIPAA") and California Civil Code § 1798.91.[21] Compl. ¶¶ 332-37; *see also* ¶¶ 207-34. Plaintiffs do not assert *claims* under these statutes, and for good reason—neither provides for a private right of action. *See Webb v. Smart Document Sols., LLC*, 499 F.3d 1078, 1082 (9th Cir. 2007); Cal. Civ. Code § 1798.91.

In any event, HIPAA does not apply here as a matter of law, even to the four defendants that the statute and regulations may cover in other contexts.[22] First, the statute was designed to regulate the use and disclosure of protected health information only in connection with certain types of transactions. 42 U.S.C. § 1320d-2(a)(1), (2). These specific transactions are listed in detail in the governing regulations, and include "health care claims or equivalent encounter

---

efforts to give them medical care during the extrication, and their transport to the hospital," and broadcast the events on a documentary); *Miller v. Nat'l Broad. Co.*, 187 Cal. App. 3d 1463, 1470 (1986) (TV crew entered the home of a man who had suffered a heart seizure and later died, filmed the work of the paramedics, and then used the film in its nightly news program).

[20] *Compare Jeffrey H. v. Imai, Tadlock & Keeney*, 85 Cal. App. 4th 345, 350-51 (2000) (lawyers for defendant in personal-injury suit obtained medical records of plaintiff's positive HIV test results, disseminated that information, and attached it to a request to introduce evidence at an arbitration), *with People v. Martinez*, 88 Cal. App. 4th 465, 478 (2001) (no privacy claim based on use of medical records in commitment proceeding), *and Snowden v. Kemper Emp'rs Claims Servs.*, 2005 WL 2374598, at *5 (Cal. Ct. App. Sept. 28, 2005) (no privacy claim based on unlawful dissemination of medical records by claims adjuster).

[21] Plaintiffs also reference several non-healthcare-related statutes. Compl. ¶¶ 332-37. As set forth above, they have failed to state a claim for violation of the federal or California wiretap statutes. *See* pp. 18-25 *supra*. And plaintiffs do not even attempt to plead violations of the Pen Register Act or the Computer Fraud and Abuse Act. The Court should disregard these "naked assertions devoid of further factual enhancement." *Ashcroft v. Iqbal*, 556 U.S. 662, 679 (2009).

[22] The complaint recognizes that Facebook, ACS, ASCO, and MRF are not "covered entities" and are therefore not subject to HIPAA. Compl. ¶ 214; *see* 45 C.F.R. § 160.103.

information," "health care payment and remittance advice," and "health care claim status." 45 C.F.R. § 160.103. Plaintiffs' claims, which arise from their browsing for health-related information on defendants' public websites, touch on none of these matters.

Second, HIPAA restricts only a covered entity's use or disclosure of "protected health information," which must be "individually identifiable." *Id.* The URLs alleged in plaintiffs' complaint do not qualify—they contain no names, addresses, birthdates, social security numbers, or any other information that a third party could use to identify the plaintiffs. Indeed, it is not even clear whether the individuals were searching for information related to their own health condition or conducting research for a term paper.

Third, the regulations define the term "individual" to mean "the person who is the subject of the protected health information." *Id.* As stated above, plaintiffs purport to bring their HIPAA-based claims without regard to whether the searches they allegedly conducted involved their own personal health-related information, and plaintiff Jane Doe II openly concedes that hers did not. *See* Compl. ¶¶ 175-76, 188, 235.[23]

More fundamentally, even if plaintiffs had alleged a violation of these statutes, they would not support a negligence per se "claim," because there is no such thing. "[T]he doctrine of negligence per se is not a separate cause of action"; instead, it "creates an *evidentiary presumption* that affects the standard of care in a cause of action for negligence." *Das v. Bank of Am., N.A.*, 186 Cal. App. 4th 727, 737-38 (2010) (emphasis added); *see* Cal. Evid. Code § 669(a); *Johnson v. Honeywell Int'l, Inc.*, 179 Cal. App. 4th 549, 558 (2009); *Quiroz v. Seventh Ave. Ctr.*, 140 Cal. App. 4th 1256, 1285 (2006). Plaintiffs cannot state a negligence claim merely by alleging a violation of various statutes; they had to allege *each* of the elements of a traditional negligence action: that (1) the "defendant had a duty to use due care," (2) "he

[23] Plaintiffs' reliance on California Civil Code § 1798.91 is also misguided. That provision—which has been mentioned in only a single reported case that did *not* involve a claim asserted under the statute, *see WorldMark v. Wyndham Resort Dev. Corp.*, 187 Cal. App. 4th 1017, 1034 (2010)—provides that "[a] business may not *request in writing* medical information *directly from an individual*." Cal. Civ. Code § 1798.91(c) (emphases added).

breached that duty," and (3) "the breach was the proximate or legal cause of the resulting injury." *Nally v. Grace Cmty. Church*, 47 Cal. 3d 278, 292 (1988); *see Johnson*, 179 Cal. App. 4th at 558 (plaintiff who relies on negligence per se "still has the burden of proving causation"). Plaintiffs do not attempt to allege either a duty or a breach. And although they claim an injury (Compl. ¶ 337), it is a purely economic harm that is not cognizable on a negligence theory under California law. *See iPhone*, 844 F. Supp. 2d at 1064. This "claim" should be dismissed.

**5. Plaintiffs Fail to State a Claim Against the Healthcare Defendants for Negligent Disclosure of Confidential Information.**[24]

The Court should dismiss plaintiffs' separate negligence claim against the healthcare defendants because plaintiffs have failed to allege either that these defendants breached a duty that they owed to plaintiffs or that harm resulted from any such breach.

First, the healthcare defendants undertook no duty to refrain from disclosing the referer headers at issue to Facebook. *See Wynne v. Orcutt Union Sch. Dist.*, 17 Cal. App. 3d 1108, 1110 (1971) (dismissing claim for negligent disclosure of information allegedly disclosed "in strict confidence," in part because "the complaint says nothing about . . . any promise . . . not to reveal" the information). To the contrary, the healthcare defendants expressly notified users that "[i]nformation you submit may be routinely shared." Compl. ¶ 171. For example, ASCO's Privacy Policy makes clear that the referer headers of pages that users view when they visit the Cancer.net website may be collected by third parties. *Id.* Ex. G, §§ 4, 13. AHS's Privacy Policy advises that it uses cookies, and that although it has taken reasonable steps to protect the security of information, "[AHS] cannot guarantee security." *Id.* Ex. I at 4; s*ee also id.* ¶ 171 (BJC Privacy Statement: "Information you submit may be routinely shared with . . . organizations working on our behalf. . . . The first visit you make to the Barnes-Jewish Hospital Web site places a 'cookie' on your computer. . . . Click here to learn more about opting out of data collection."); *id.* Ex. K at 3 (Cleveland Clinic Privacy Policy makes "no guarantee as to security, integrity or confidentiality of any information transmitted to or from this website, or stored

[24] The following two claims are asserted only against the healthcare defendants. The final three claims discussed below are asserted only against Facebook.

within this website"); *id.* Ex. H (MRF's privacy policy describes use of cookies, and states that it does "not control, operate or endorse in any respect" third-party sites with links on MRF's site).

Second, as stated above, HIPAA's restrictions against disclosure of "protected health information" (*see* Compl. ¶ 339) have no relevance here, because public URLs are not protected health information. *See* p. 29 *supra*; 45 C.F.R. § 164.514(a); 42 U.S.C. § 1320d. Every court that has considered HIPAA's disclosure restriction has confirmed that it does not regulate public information unrelated to a patient's identity or health, such as the referer headers at issue here,[25] which could not reasonably "be used to identify" any of the named plaintiffs.[26] Plaintiffs' generalized allusions to HIPAA simply cannot transform the URLs at issue into "sensitive health information." After all, people can—and frequently do—seek information about cancer and other health conditions for reasons entirely unrelated to their own medical condition.

Third, plaintiffs have failed to allege an injury proximately caused by the healthcare defendants' conduct. They simply allege in conclusory fashion that they were "harmed by having their sensitive medical-information disclosed," and "suffered damage in that what [they] intended to remain private is no longer so." Compl. ¶¶ 337, 342. These allegations are insufficient. *See, e.g.*, *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 962-63 (S.D. Cal. 2012) (dismissing negligence claim for failure to allege injury caused by data breach, notwithstanding plaintiffs' allegations of exposure to an increased risk of

---

[25] *See, e.g.*, *Jackson v. Jamaica Hosp. Med. Ctr.*, 61 A.D. 3d 1166, 1167, 1169 (N.Y. App Div. 2009) (a patient's "'time of arrival' at [an] emergency room and 'time of death'" does not constitute protected health information because "it has no apparent connection to the victim's physical condition or medical care"); *Shannon A. v. Orland Unified Sch. Dist.*, 2012 WL 1552538, at *1-2 (E.D. Cal. Apr. 30, 2012) (doctor's disclosure "that his records showed that he had not seen [plaintiff]" "do[es] not support drawing a reasonable inference that [the doctor] disclosed information" protected by HIPAA); *State ex rel. Cincinnati Enquirer v. Daniels*, 844 N.E.2d 1181, 1185 (Ohio 2006) (a "nondescript reference to 'a' child with 'an' elevated lead level" does not constitute "health information" under HIPAA); *Foley v. Samaritan Hosp.*, 11 Misc. 3d 1055(A), at *2 (N.Y. Sup. Ct. 2006) (disclosure of the name of a hospital patient, without reference to the medical treatment he or she received, does not violate HIPAA); *Rogers v. NYU Hosps. Ctr.*, 795 N.Y.S.2d 438, 441 (Sup. Ct. 2005) (same).

[26] That is particularly true of BJC and Cleveland Clinic because, as discussed above (at p. 13 n.6), plaintiffs do not allege that Jane Doe II communicated any of her own health information to their websites. *See* Compl. ¶¶ 175-76, 188.

identity theft and fraud); *Regents of Univ. of Cal. v. Super. Ct.*, 220 Cal. App. 4th 549, 554, 570 (2013) (dismissing claim for negligent disclosure of "patient names, dates of birth, addresses, financial information and medical records" because plaintiffs could not allege resulting misuse of the disclosed information).

**6. Plaintiffs Fail to State a Claim Against the Healthcare Defendants for Breach of the Fiduciary Duty of Confidentiality.**

Plaintiffs' claim against the healthcare defendants for breach of fiduciary duty fails for the same reasons. That claim requires plaintiffs to allege (1) the existence of a fiduciary relationship, (2) a breach of that duty, and (3) resulting harm. RESTATEMENT (SECOND) OF TORTS § 874 (1979). It takes more than visiting an entity's website to establish a legally enforceable fiduciary relationship. As set forth above, neither the healthcare defendants' privacy policies nor any other source of authority supports plaintiffs' allegation that they owed or breached a duty to plaintiffs, much less a fiduciary duty. *See* Compl. ¶¶ 343-47. And, again, plaintiffs have failed to allege any actual, particularized, harm caused by defendants' alleged conduct.

**7. Plaintiffs Fail to State a Claim for Breach of the Duty of Good Faith and Fair Dealing Against Facebook.**

Plaintiffs claim that Facebook violated the "duty of good faith and fair dealing in its performance and enforcement" of the SRR, Data Policy, and Cookie Policy. Compl. ¶¶ 350-55. This claim fails because Facebook fully complied with these disclosures and plaintiffs have not alleged any facts to the contrary. *See* pp. 16-18 *supra*. It also fails because it is based solely on Facebook's alleged breach of the underlying contracts (*id.* ¶ 355) and is thus not separately cognizable under California law. *Partti v. Palo Alto Med. Found. for Health Care, Research & Educ., Inc.*, 2015 WL 6664477, at *5 (N.D. Cal. Nov. 2, 2015) ("If the allegations do not go beyond the statement of a mere contract breach . . . , they may be disregarded . . . .").

**8. Plaintiffs Fail to State a Claim for Fraud Against Facebook.**

Plaintiffs' action for fraud under Sections 1572 and 1573 of the California Civil Code (Compl. ¶¶ 363-68) is frivolous. A fraud claim has five elements: "(a) a misrepresentation (false

representation, concealment, or nondisclosure); (b) knowledge of falsity (or 'scienter'); (c) intent to defraud, *i.e.*, to induce reliance; (d) justifiable reliance; and (e) resulting damage." *In re Estate of Young*, 160 Cal. App. 4th 62, 79 (2008). Rule 9(b) requires that "the circumstances constituting fraud" be alleged with "particularity." Fed. R. Civ. P. 9(b).

Plaintiffs allege only that Facebook "suppress[ed], with intent to deceive its users," facts about its collection and use of health-related communications, and that they "relied on Facebook's false assertions in contracting with and using Facebook." Compl. ¶ 366. These bare conclusions do not satisfy Rule 12(b)(6), let alone Rule 9(b). First, Facebook made no misrepresentation; its disclosures were accurate and complete. *See* pp. 16-18 *supra.* Second, plaintiffs do not allege that Facebook acted with intent to *induce plaintiffs* to take any action; the claim that Facebook had a generalized "intent to deceive its users" (Compl. ¶ 366) is both groundless (*see* pp. 16-18 *supra*) and legally insufficient.[27] Third, plaintiffs have not alleged that absent the alleged misrepresentations, they "would not, in all reasonable probability, have entered into the contract," *Engala v. Permanente Med. Grp., Inc.*, 15 Cal. 4th 951, 976 (1997), or that any reliance was "justifiable" in light of Facebook's disclosures, *Young*, 160 Cal. App. 4th at 79. And finally, plaintiffs do not claim damage at all, let alone *as a result of the alleged fraud. See Moncada v. W. Coast Quartz Corp.*, 221 Cal. App. 4th 768, 776 (2013); *Marble Bridge Funding Grp. v. Euler Hermes Am. Credit Indem. Co.*, 2015 WL 971761, at *5 (N.D. Cal. Mar. 2, 2015).[28]

[27] *See Blickman Turkus, LP v. MF Downtown Sunnyvale, LLC*, 162 Cal. App. 4th 858, 869 (2008) ("It is not enough that the misstatement (or concealment) actually harmed the plaintiff; it must have been made by the defendant with the intent to *induce action* (or inaction) by the plaintiff."); *Levin v. Citibank, N.A.*, 2009 WL 3008378, at *5 (N.D. Cal. Sept. 17, 2009); *Senah, Inc. v. Xi'an Forsar S & T Co.*, 2014 WL 3044367, at *4 (N.D. Cal. July 3, 2014).

[28] Plaintiffs' "constructive fraud" claim (Compl. ¶ 367) fails for the additional reason that they did not allege that Facebook had a duty to speak, which would be the case only if it had a "fiduciary or confidential" relationship with them. *Dealertrack, Inc. v. Huber*, 460 F. Supp. 2d 1177, 1183 (C.D. Cal. 2006).

**9. Plaintiffs Have No Claim Against Facebook for Quantum Meruit.**

Plaintiffs claim that "Facebook obtained a benefit" from its collection of data and "may not justly retain th[is] benefit." Compl. ¶¶ 370-71. They refer to this claim as "quantum meruit" *id.* at p. 84), which is also known as "unjust enrichment." *See Maglica v. Maglica*, 66 Cal. App. 4th 442, 449 (1998). But like negligence per se, "[u]njust enrichment is not a cause of action." *Hill v. Roll Int'l Corp.*, 195 Cal. App. 4th 1295, 1307 (2011); *see also Gabali v. Onewest Bank, FSB*, 2013 WL 1320770, at *7 (N.D. Cal. Mar. 29, 2013) (Davila, J.). Plaintiffs also do not allege the absence of an enforceable agreement, as required for a quantum meruit theory. *See Klein v. Chevron U.S.A., Inc.*, 202 Cal. App. 4th 1342, 1389 (2012). Nor do plaintiffs' allegations show how Facebook's conduct—its receipt of referer headers in the normal course of operation of the Internet—was "unjust," or how any "unjust benefit was retained at plaintiffs' expense." *In re Actimmune Mktg. Litig.*, 2009 WL 3740648, at *16 (N.D. Cal. Nov. 6, 2009).

**CONCLUSION**

The complaint should be dismissed with prejudice.

Dated: June 30, 2016

MAYER BROWN LLP

By: /s/ John Nadolenco
JOHN NADOLENCO, State Bar No. 181128
jnadolenco@mayerbrown.com
350 South Grand Avenue, 25th Floor
Los Angeles, California 90071-1503
Telephone: (213) 229-9500
Facsimile: (213) 625-0248

LAUREN R. GOLDMAN*
lrgoldman@mayerbrown.com
1221 Avenue of the Americas
New York, NY 10020-1001
Telephone: (212) 506-2500
Facsimile: (212) 262-1910

**Admitted pro hac vice*

*Attorneys for Defendant*
*FACEBOOK, INC.*

WILSON SONSINI GOODRICH & ROSATI
Professional Corporation

By: /s/ Michael H. Rubin
MICHAEL H. RUBIN, State Bar No. 214636
mrubin@wsgr.com
PETER C. HOLM, State Bar No. 299233
pholm@wsgr.com
1 Market Street
Spear Tower, Suite 3300
San Francisco, CA 94105
Telephone: (415) 947-2000
Facsimile: (415) 947-2099

ANTHONY J WEIBELL, State Bar No. 238850
aweibell@wsgr.com
LAUREN GALLO WHITE, State Bar No. 309075
lwhite@wsgr.com
650 Page Mill Road
Palo Alto, CA 94304
Telephone: (650) 493-9300
Facsimile: (650) 565-5100

*Attorneys for Defendant*
*BJC HEALTHCARE*

HOLLAND & KNIGHT LLP

By: /s/Shelley G. Hurwitz
SHELLEY G. HURWITZ, State Bar No. 217566
400 S. Hope St., 8th Floor
Los Angeles, CA 90071
Telephone: (213) 896-2400
Facsimile: (213) 896-2450

JOHN P. KERN, State Bar No. 206001
DAVID I. HOLTZMAN, State Bar No. 299287
50 California Street, Suite 2800
San Francisco, CA 94111
Telephone: (415) 743-6900
Facsimile: (415) 743-6910

STEVEN B. ROOSA*
31 West 52 Street
New York, NY 10019
Telephone: (212) 513-3544
Facsimile: (212) 513-3544

*Attorneys for Defendants*
*ADVENTIST HEALTH SYSTEM SUNBELT HEALTHCARE CORPORATION (SUED AS "ADVENTIST HEALTH SYSTEM");*
*AMERICAN CANCER SOCIETY, INC.; AND*
*MELANOMA RESEARCH FOUNDATION*

**Pro hac vice application to be filed*

JONES DAY

By: /s/ Jeffrey Rabkin
JEFFREY RABKIN, State Bar No. 189798
jrabkin@jonesday.com
BRANDY H. RANJAN*
branjan@jonesday.com
ALEXANDRA A. MCDONALD, State Bar No. 300950
amcdonald@jonesday.com
555 California Street, 26th Floor
San Francisco, CA 94104
Telephone: (415) 875-5850
Facsimile: (415) 875-5700

* *Admitted pro hac vice*

BRIAN G. SELDEN, State Bar No. 261828
bgselden@jonesday.com
1755 Embarcadero Road
Palo Alto, CA 94303
Telephone: (650) 739-3939
Facsimile: (650) 739-3900

*Attorneys for Defendant*
*AMERICAN SOCIETY OF CLINICAL ONCOLOGY, INC.*

BAKER & HOSTETLER LLP

By: /s/ Teresa Chow
TERESA CHOW, State Bar No. 237694
tchow@bakerlaw.com
11601 Wilshire Boulevard, Suite 1400
Los Angeles, CA 90025-0509
Telephone: (310) 820-8800
Facsimile: (310) 820-8859

STEVEN M. DETTELBACH*
sdettelbach@bakerlaw.com
DANIEL R. WARREN*
dwarren@bakerlaw.com
DAVID A. CARNEY*
dcarney@bakerlaw.com
127 Public Square, Suite 2000
Cleveland, OH 44114-1214

* *Pro hac vice application to be filed*

*Attorneys for Defendant*
*CLEVELAND CLINIC*

BAKER & HOSTETLER LLP

By: /s/ Teresa Chow
TERESA CHOW, State Bar No. 237694
tchow@bakerlaw.com
11601 Wilshire Boulevard, Suite 1400
Los Angeles, CA 90025-0509
Telephone: (310) 820-8800
Facsimile: (310) 820-8859

PAUL G. KARLSGODT*
pkarlsgodt@bakerlaw.com
CASIE COLLIGNON*
ccollignon@bakerlaw.com
1801 California Street, Suite 4400
Denver, CO 80202-2662
Telephone: (303) 861-0600
Facsimile: (303) 861-7805

* *Admitted pro hac vice*

*Attorneys for Defendant*
*UNIVERSITY OF TEXAS—MD*
*ANDERSON CANCER CENTER*

**ATTESTATION**

I, John Nadolenco, hereby attest, pursuant to N.D. Cal. Local Rule 5-1(i)(3), that concurrence to the filing of this document has been obtained from each signatory.

By: */s/ John Nadolenco*
John Nadolenco